AUSTRALIAN COMMISSION ON SAFETY AND QUALITY IN HEALTH CARE

National Safety and Quality Digital Mental Health Standards

ACTION GUIDE – FOR DIGITAL MENTAL HEALTH SERVICE PROVIDERS

Clinical and Technical Governance Standard:

Information security management systems

Digital mental health service providers hold many types of valuable information, including sensitive personal and clinical health information. Healthcare is a target for cybercriminals because of the value and quantity of personal data held; good information security practice is therefore vital.

Information security deals with information assets and the protection of data from any form of threat. It should provide confidentiality, integrity, and availability for users and protect information from unauthorised access, data modification and removal.

What is an information security management system?

An information security management system is a structured and systematic approach to managing information security and other IT-related risks. It includes wide-ranging controls to keep data secure from diverse security threats and vulnerabilities. It can help to assure general information security, as well as personal data protection.

The International Organization for Standardization (ISO) has developed ISO 27001, a standard that provides a structured methodology dedicated to information security and the requirements for an information security management system. According to ISO 27001 the system should address:

- The relevant stakeholders for the service and their expectation for information security
- The risks for the information being handled by the service
- The safeguards and procedures in place to mitigate or manage risks
- The service's information security objectives
- The process for measuring the effectiveness of safeguards and risk management procedures
- Strategies for continuous improvement of the information security management system.

Action in the NSQDMH Standards

Information security is addressed in **Action 1.35** of the National Safety and Quality Digital Mental Health (NSQDMH) Standards which requires service providers to have an information security management system in place that protects the security and stability of the data held by a digital mental health service.

Risks, threats and vulnerabilities

It can be helpful to define some of the key terms used when discussing information security. According to the Australian Cyber Security Centre, **a security risk** to an information security management system is any event that could result in the compromise, loss of integrity or unavailability of data or resources, or deliberate harm to people measured in terms of its likelihood and consequences.

A **cyber threat** is any circumstance or event with the potential to harm systems or data. **Security vulnerability** is a weakness in a system's security requirements, design, implementation or operation that could be accidentally triggered or intentionally exploited and result in violation of the system's security policy.

Below are some examples of potential threats and vulnerabilities. It is important to note that threats can be both intentional and unintentional.

Threats

- Malicious actors using software including ransomware, malware or phishing attacks
- Trusted insiders performing unauthorised access
- Damage resulting from testing
- Electricity failure
- Equipment malfunction
- Loss or destruction of records
- Misconfigurations leaking sensitive data
- Maintenance errors
- Software errors
- Theft
- User error

> **Top tip**: *The Department of Industry, Science, Energy and Resources has developed a Cyber Security Assessment Tool to help businesses assess their cyber security strengths and areas for improvement.*

Vulnerabilities

Staff:

- Inadequate segregation of duties and segregation of operational and testing facilities
- Inadequate supervision or training of employees
- Lack of appropriate delegation and support

Systems management:

- Inadequate or irregular backup
- Inadequate password management
- Disposal of storage media without deleting data
- Insufficient software testing
- Lack of systems for identification and authentication
- Unprotected public network connections
- User rights not reviewed regularly
- Uncontrolled copying of data
- Undocumented software

Equipment and maintenance:

- Inadequate maintenance
- Lack of protection for mobile equipment
- Out of date equipment

Cyber security roles

Service providers should have appropriate cyber security roles in place, staffed by individuals with the appropriate skills and competencies, or who are able to access appropriate advice via external agencies or consultants. The Australian Cyber Security Centre recommends that organisations appoint a Chief Information Security Officer or delegate a staff member with the overall responsibility of providing cybersecurity leadership and guidance. The Chief Information Security Officer is responsible for overseeing their organisation’s cyber security program and ensuring compliance with cyber security policy, standards, regulations and legislation. The Chief Information Security Officer should adopt a continuous approach to learning and upskilling in order to keep pace with evolving technologies and threats.

> **Top tip**: *The Information Security Manual published by the Australian Cyber Security Centre provides detailed guidance on applying a cybersecurity framework, using a risk management approach and protecting systems and data from cyber threats.*

Risk assessment and action plan

A critical step in developing an information security management system is to undertake a risk assessment of the likely threats the service may face. It is important for the service as a whole to agree on the parameters of the risk assessment, including how risk will be measured, what is encompassed (for example, both direct loss of an asset as well as reputational harm), and what is considered to be an acceptable level of risk.

Service providers should list all their information assets and the impact and likelihood of the associated risks to those assets. Service providers should also agree who is responsible for owning the risk and ensure that person has the skills and competency or can access appropriate support to respond effectively to these risks.

Information system assets

- Hardware: laptops, servers, printers and mobile phones
- Software
- Information including databases and files
- Infrastructure including offices, electricity and air-conditioning
- Staff
- Services such as legal services, DropBox, etc.

Once a list of assets and risks are identified, providers are able to rate each risk according to its level of severity and determine the action to be taken. The Australian Cyber Security Centre *Information Security Manual* includes advice on IT controls that can be applied to help minimise and mitigate a number of cyber security risks.

Service providers should ensure they have documented all the actions taken in a risk assessment and action report detailing who is responsible for implementing actions, the expected time frame for implementation and the budget allowed.

ISM risk management framework

The *Information Security Manual* outlines six key steps in its risk management framework. Note: The framework should be in place before a service commences operation.

1. **Define the system –** Determine the type, value and security objectives for the system based on an assessment of the impact if it were to be compromised
2. **Select controls** – Select controls for the system and tailor them to achieve desired security objectives
3. **Implement controls** – Implement controls for the system and its operating environment
4. **Assess controls –** Assess controls for the system and its operating environment to determine if they have been implemented correctly and are operating as intended
5. **Authorise the system** – Authorise the system to operate based on the acceptance of the security risks associated with its operation
6. **Monitor the system** – Monitor the system, and associated cyber threats, security risks and controls, on an ongoing basis

Detecting and managing incidents

Cyber threats continue to evolve and it can be challenging to maintain ongoing security. The *Information Security Manual* provides guidance on how to prepare for and manage a cyber security incident. This includes:

- How to write an incident management policy and develop an incident register
- How to handle and contain data spills
- How to handle and contain malicious code infections
- How to handle and contain intrusions
- How to ensure the integrity of evidence collected following a cyber security incident.

In addition, the guide, *Windows Event Logging and Forwarding* provides advice on setting up systems to detect and investigate malicious activity.

The Essential Eight Maturity Model

The Australian Cyber Security Centre has developed eight essential strategies to help cyber security professionals mitigate cyber security incidents. These baseline strategies, known as the Essential Eight, make it harder for adversaries to compromise systems.

1. Application control – prevent the execution of scripts, installers, etc. in specific circumstances
2. Patch applications – apply promptly and use a vulnerability scanner to identify missing updates
3. Configure MS Office macro settings – disable for users who do not have a demonstrated business requirement
4. User application hardening – for example, prevent web browsers from processing Java and advertisements from the internet
5. Restrict administrative privileges
6. Patch operating systems promptly and scan for missing updates
7. Multi-factor authentication
8. Regular back-ups

Summary: Developing an information security management system

Issue

Protecting the security and stability of the data held by a digital mental health service

Solution

Appoint a Chief Information Security Officer, undertake a risk assessment, develop a risk management framework

Barriers

Lack of staff with appropriate skills and competencies, resourcing, evolving technologies

Enablers

Appointing expert consultants, accessing resources from the Australian Cyber Security Centre, monitoring and reviewing risk assessment

Find out more

Service providers seeking further information and useful guidance on information security should access resources produced by the Australian Cyber Security Centre.

You can learn more about the NSQDMH Standards and other supporting resources at safetyandquality.gov.au/DMHS.

Contact the digital mental health program team at DMHS@safetyandquality.gov.au.

safetyandquality.gov.au